KEYper® Electronic Key System

Users Manual for Security

Rev. 2 21 April 2010

1-800-399-7888

Contents

Introduction

Familiarization

The **KEYper® Systems** electronic key system is an investment in key management, control and accountability. A properly used and maintained system will provide owners, managers and users the ability to track key movements as well as make accurate user and key data available.

It is important for key system administrators to become very familiar with the key system, both the hardware and the software. It should be the administrators' responsibility to perform regular maintenance on the system as well as train users and other administrators.

A key system is comprised of several hardware components. Among these are the:

- **system controller - includes computer, keyboard, mouse and monitor (1 per system)**
- **key cabinet(s) – includes stand(s) or wallboard(s)**
- **cabinet controller - (1 per cabinet)**
- **communication board - (1 per cabinet)**
- **I-button, or Fob, reader assembly – includes cradle; DS9490 adapter (1 per system)**
- **biometric, or Fingerprint, reader** - (1 per system)**
- **battery backup - (1 per system)**

All key system administrators should be able to identify these components and be aware of their placement with regard to user access *and* component security.

The key management program runs on the system controller and interfaces with the fob and fingerprint readers, the communication board (or radios if your system is configured for RF) and the cabinet controller. The system controller sends commands to, and receives responses from, the cabinet controller via a serial connection (or, again, wireless radio frequency if your system is configured for RF). The program offers a variety of views and reports, simple **Check In** and **Check Out** procedures and of course, a range of administrative tools. The system is designed to automatically log a user off after every transaction or if a timeout has expired.

Always allow the traffic light icon in the lower right corner of the task bar to turn green before starting the **KEYper® software. Please follow the instructions included in the user manual regarding maintenance of the biometric device

Maintenance

As with any piece of equipment, the key system requires regular maintenance. The maintenance required consists mainly of keeping the **View Assets Out** file cleansed of all assets no longer in inventory. Keeping the system clean, particularly the computer tower cooling fans and vents, and rebooting the system at least once a week will promote system health..

System Reboot Procedure

The procedure for a complete system reboot consists of removing power from the cabinet(s) and performing a normal shutdown of the computer. After a few minutes restore power to the cabinet(s) and restart the computer. Give the cabinets and fingerprint reader a few minutes to completely configure before restarting the **KEYper®** program.

The biometric fingerprint reader lens has a clear, rubber-like protective cover. The best method for cleaning the lens is to place transparent tape (ex., Scotch) on the lens and peel it off. This will generally remove built up dirt, grime, oils, etc. This should be accomplished at least once per week. In maintenance areas where undesired build-up is more prevalent, clean the lens more often.

Conventions

Throughout this manual, important information and items of note are designed to draw the reader's attention and marked with an *asterisk, in **bold type**, in *italics*, underlined, highlighted or some combination thereof.

Instructions, such as **Login > Admin > User**, are simply shorthand for, **"Log into the software, select Admin and then select User"**.

All time entries may be made using the 24-hour clock format.

***!IMPORTANT!* NEVER LOAD OTHER SOFTWARE ON THE KEY SYSTEM CONTROLLER. SENSITIVE SYSTEM FILES MAY BECOME CORRUPT IF EXPOSED TO INCOMPATIBLE APPLICATIONS. THIS MAY ALSO VOID THE WARRANTY AGREEMENT.**

Installing Fobs & Tamper Seals

(Figs. A – D)

The fob is a very integral part of the system. Each fob contains a chip with a unique series of digits, which is associated with vehicle or other data when the key is entered into the system. Fobs can be reused over and over. Each cabinet is shipped with a full compliment of fobs and, barring theft, loss or damage, they rarely require replacement. ***Do not place wet fobs in the cabinet***. Dry the fob button before placing it in the cabinet. Periodically inspect fobs for obvious damage.

It is highly recommended that a small bucket, box or other container be used for holding fobs awaiting deletion. When a vehicle has been sold, traded or is otherwise no longer in inventory, remove the tamper seal with a pair of side cutters (wire cutters, dykes, etc) and throw it away. The vehicle data associated with the fob must be deleted **(see Identify Fob, pg. 7)**, and then the fob can be re-used.

It is recommended the **tamper seal (Fig. A)** be installed through the key as illustrated in **Fig. B**, or through the "hard part" of the key. Install the **fob** as illustrated in **Fig. C.** Insert the open end of the **tamper seal** into the slot in the tab until locked. The preferred result is shown in **Fig. D**. It is further recommended only the minimum required to demonstrate the vehicle be attached to the tamper seal and fob.

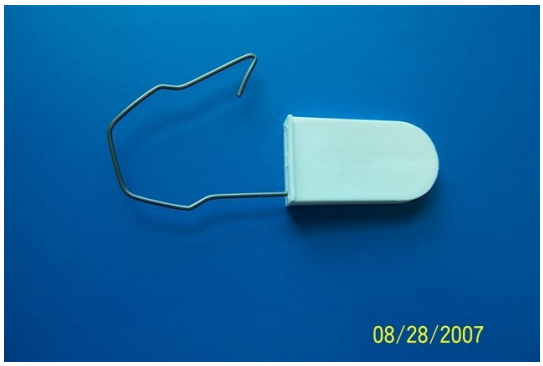


Fig. A

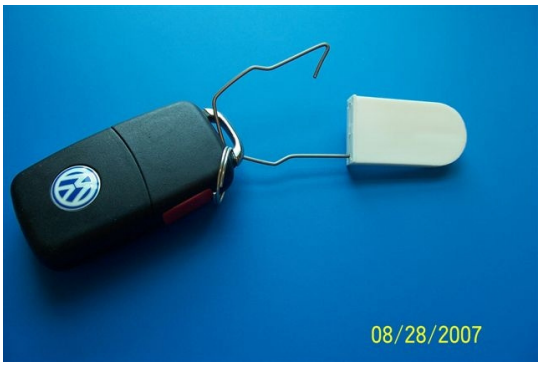


Fig. B

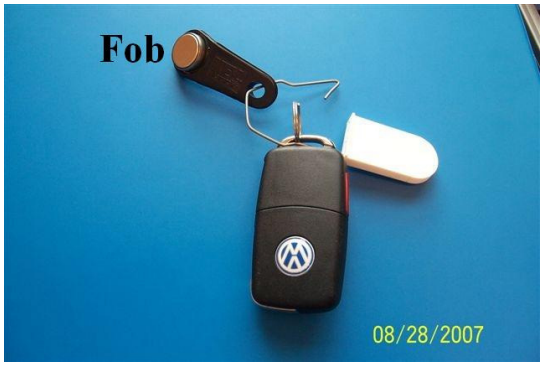


Fig. C

Fig. D

SECTION I: Quick Reference

The screen shown in **Fig. 1** is the main, or login screen for Keyper® Automotive software. The version operating on your system is indicated at the top of the screen. It is from here that all other functions are accessed. A user will log in with a password or a fingerprint depending on **Login Options** setting. **(See pg. 13)** **Fig. 1** illustrates the "*either/or*" option.

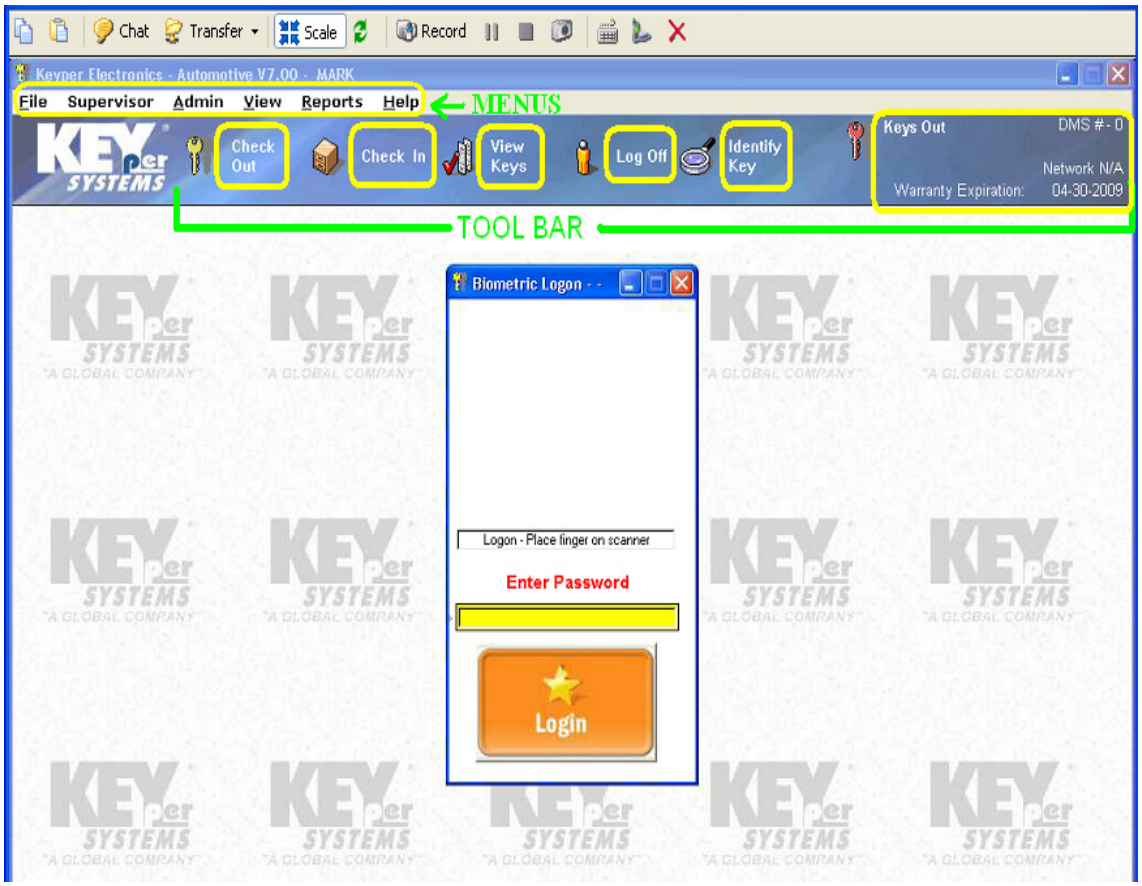


Fig. 1

The toolbar area contains five functions and some system information, identified here by yellow boxes. Use **Check Out** and **Check In** to remove and return keys. **View Assets** displays your local asset database or, if your system is networked with other key systems, the asset databases for all systems are displayed. Click **Log Off** any time it is displayed on the toolbar to exit to the login screen. **Identify Fob** will display what, if any, information is in the asset database associated with the fob you are identifying.

At the far right of the toolbar are reference displays; Asset**s Out** simply lets you know at a glance that there are assets currently checked out of the system. If your system is networked with other key systems, the status of the network is displayed. This is also where the "**Unknown Fobs Found**" message is displayed. **(See pg. 19)** Finally, the expiration date of the initial system warranty is displayed for your convenience. Identified in the upper left area of the login screen are six menus.

Identify Fob **(Login > Identify Fob)**

(Also see previous page: Identify Fob)

If you have a fob in hand, with keys (asset) attached, but are unsure of the identity of the asset, use this function as an aid to identifying the asset. Select **Identify Fob** from the toolbar, hold the fob on the fob reader and click **ID Key**. If the fob is associated with an asset and has been properly entered in the system, that asset information will be displayed. You may also delete an asset from your inventory by selecting **Delete**.

Checking Assets Out **(Login > Check Out)**

(Figs. 2-3)

Before checking keys out, you should understand the sorting and searching features of the **Issue Keys** window. First, a column is highlighted in **red** by clicking on a column header, such as **Asset ID**. That tells the system to sort the key database by **Asset ID** *and* the search criterion is now based on asset ID's.

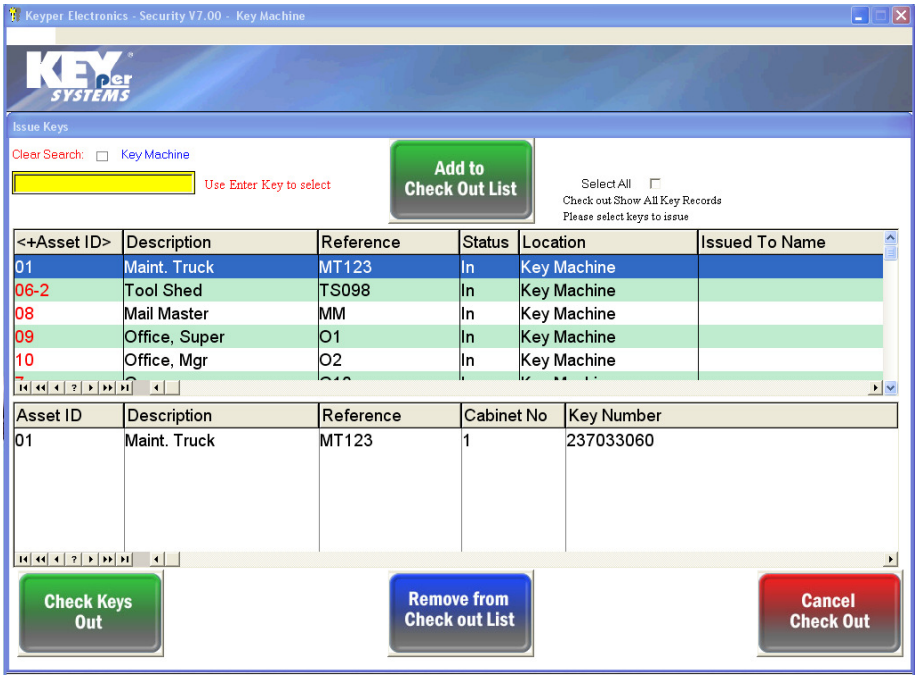


Fig. 2

That is to say, with a search criterion of **Asset ID**, search entries ***must*** be **Asset ID**'s. If the **Description** column is in **red**, search entries must be asset descriptions. The computer is going to search the highlighted column for whatever is entered in the search bar. Type an entry relating to the highlighted column into the yellow search bar and press **Enter**. The key will either appear in the check out list area of the window, as in **Fig. 2**, or one of two pop-ups will appear: "**Key Not In Database"** means the requested stock number is not among those currently in the key database; or "**User: John Doe has key"** if the key is in the database, but currently checked out to another user.

Selecting Assets

There are a few ways to select assets for check out. Ensure the appropriate column is highlighted in **red**, click in the search bar to make it active, enter criteria related to the highlighted column and press **Enter**. The selection will appear in the check out list window if it is in the database and in the cabinet. Multiple selections may be made in this manner. Click **Check Keys Out**.

Other ways to select assets:

- Highlight selection and click **Add to Check Out List**. Make multiple selections in this manner. Click **Check Keys Out** when ready.
- Make multiple selections by scrolling through the assets and pressing the **CTRL** key while highlighting each selection. Click **Add to Check Out List** and **Check Keys Out**.
- Choose a block of assets by highlighting the first asset, holding the **SHIFT** key down and highlighting the last selection. All the assets from first to last will highlight. Click **Add to Check Out List** and **Check Keys Out**.

To remove a selection from the check out list, highlight the key and click **Remove from Check Out List**.

Selecting an Issue Reason

(Fig. 3)

If enabled, it is at this point in the check out process that the user will have to select a reason for removing the asset before it will be issued. Click on the arrow button for one of the available reasons. If none of those available fits the purpose, type something into the **Default Reason** bar and click the arrow. If a number of assets are being issued, select a reason for ***each*** asset as it appears in the **Key Checked Out** field, or assign the same reason to all of the assets by clicking on **Set All Keys to Same Reason** and then selecting the reason. Once the reason has been selected the cabinet door lock will fire and the exterior LED will light. Pull the cabinet open, remove the illuminated selection(s) and close the door. The system will automatically return to the login screen.

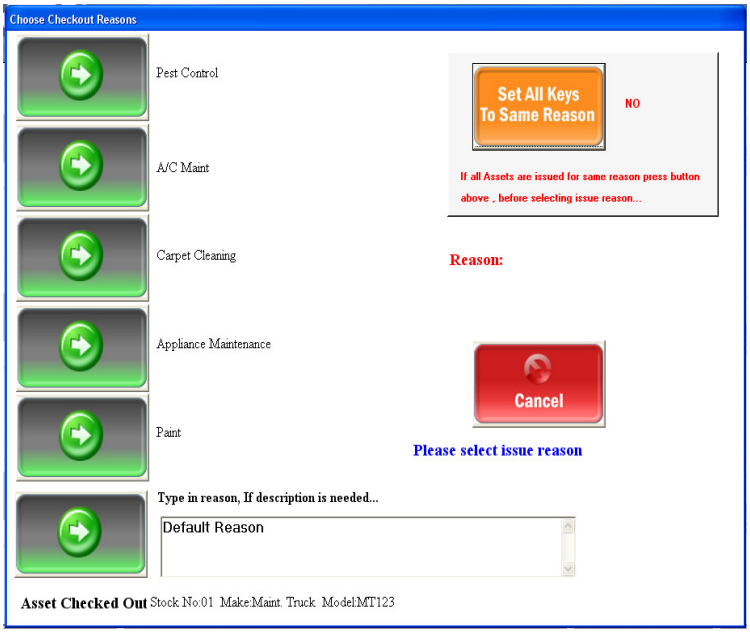


Fig. 3

***NOTE:** Once the key has been checked out, the issue reason cannot be changed.

Checking Assets In (Login > Check In)

(Fig. 4)

If the system has only one cabinet, it will fire when **Check In** is selected and the asset may be returned to any position.

If there are multiple cabinets the screen shown in **Fig. 4** will appear. Highlight a cabinet by clicking on it and then click **Check In.** Return asset(s) to any position. Assets may also be returned during a **Check Out** transaction.

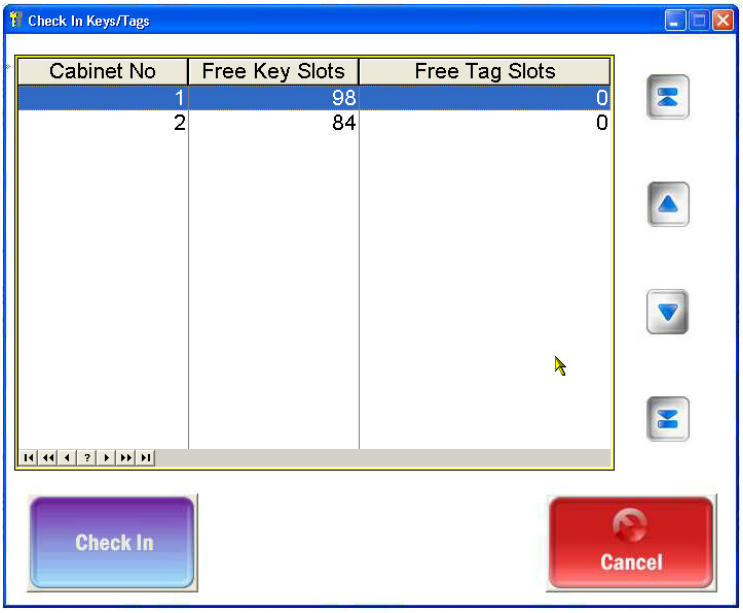


Fig. 4

Adding/Deleting Users (Login > Supervisor> Users)

(Fig. 5)

To **Add** users select **Add Record.** To **Change** the record of a user, highlight the users name and select **Change Record.** To **Delete** a user, highlight the users name and select **Delete Record**

Add a User (Fig. 5 inset)

Click **Add Record** to bring up the **Adding a User Record** screen. Required entries are marked with an asterisk

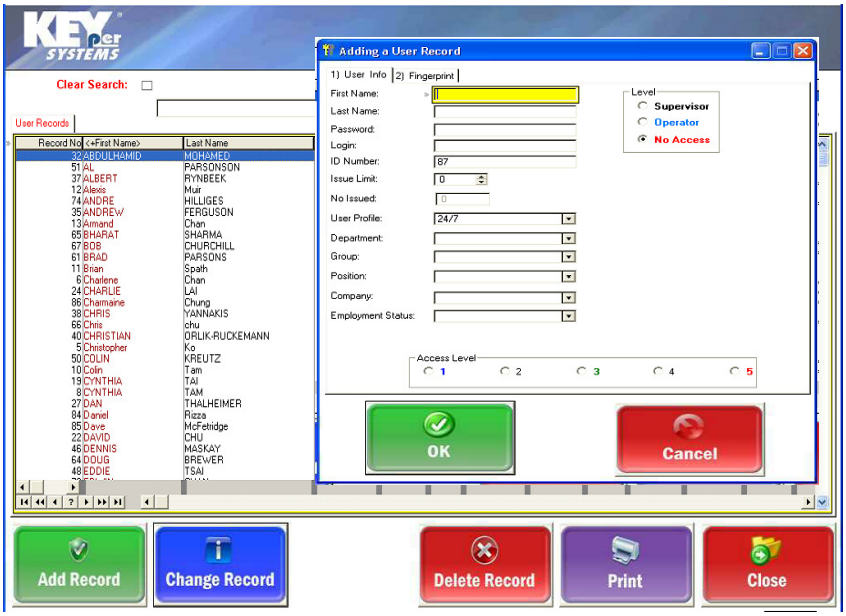


Fig. 5

*Enter the users' name

*Choose a **Password** from 4 to 12 characters

***Login** will fill automatically

*Enter an **Issue Limit** greater than 0

*Assign a **Profile** and a **Level**

***No. Issued** will display the number of keys a user currently has checked out of the system

***Access Level** will default to 3 if no choice is made. (See page 17 for more information regarding **Level** and **Access Level**)

!! Before re-adding a previously deleted user, read WARNING on next page !!

WARNING

If you are re-adding a previously deleted user, you must make a change to the users' name. (ex., John Doe becomes J. Doe or John Doe2, etc.) It is highly recommended that the user choose a different password and print a different finger.

Fingerprint Enrollment **(Login > Supervisor> Users)**

(Figs. 6-8)

NOTE: The best prints are captured by placing the chosen finger, from about the first knuckle to the tip, ***flat*** on the scanner and applying ***gentle*** pressure.

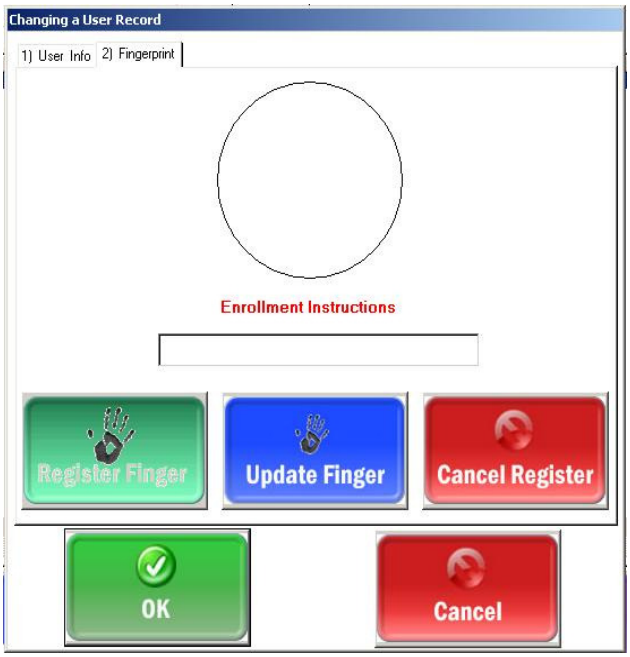


Fig. 6

Click on the **2] Fingerprint** tab at the top of the window to bring up the screen in **Fig. 3**. Whether registering a new user or reprinting an existing user, click **Register Finger** to bring up the screen shown in **Fig. 4**. If the user has never been printed, all of the fingers in the graphic will be "blank". Click on the finger the user is registering and the screen shown in **Fig. 5** will appear. The user must place his/her finger on the scanner lens, see 'NOTE' above, for four(4) acceptable scans. If any errors or "bad quality" scans occur, simply try again. Once four good scans are acquired, a message box will appear advising the print procedure was successful. Click OK. If the user has an existing fingerprint in the database, one of the fingers will be green. Click on the green finger and you will prompted to continue deleting the existing print. Select **Yes**. Then click on the finger the user will register and follow the preceding ions.

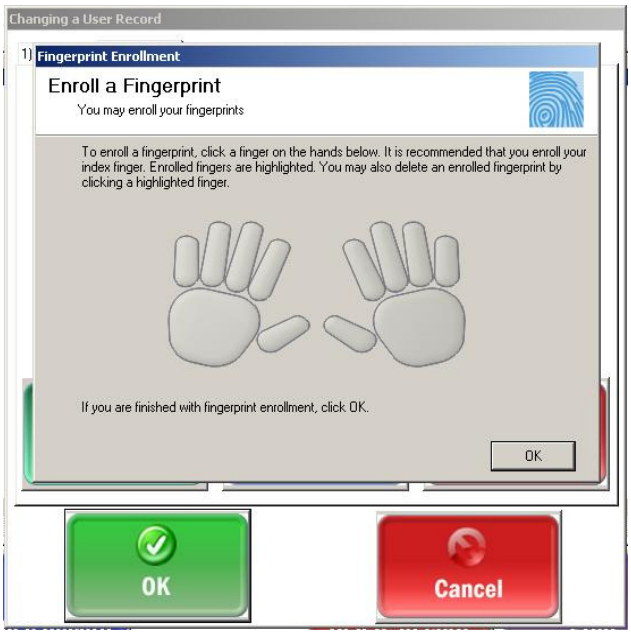


Fig. 7

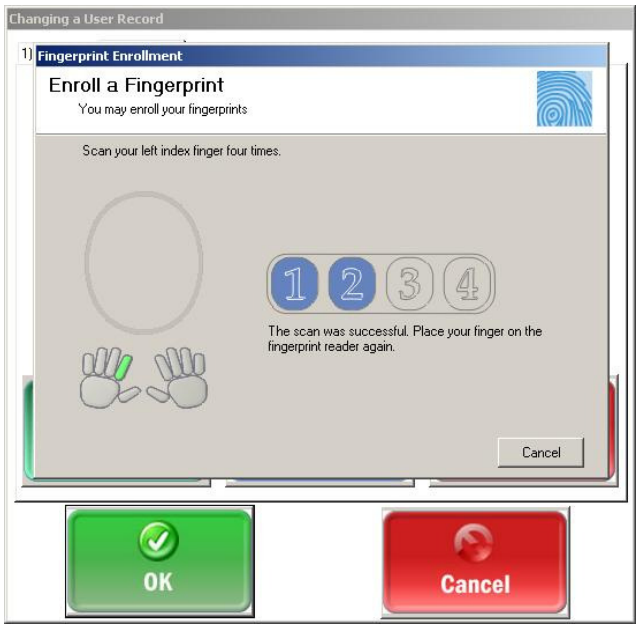


Fig. 8

Adding/Deleting Assets (Login > Admin > Assets)

(Figs. 9-11)

The screen shown in **Fig. 9** allows the addition of assets to the system, the deletion of assets, as well as changing the record of any asset. You can also print the entire asset database from here. *To delete or change an asset, highlight the asset and click the appropriate button. (see also* Identify Fob*, pg. 7)*

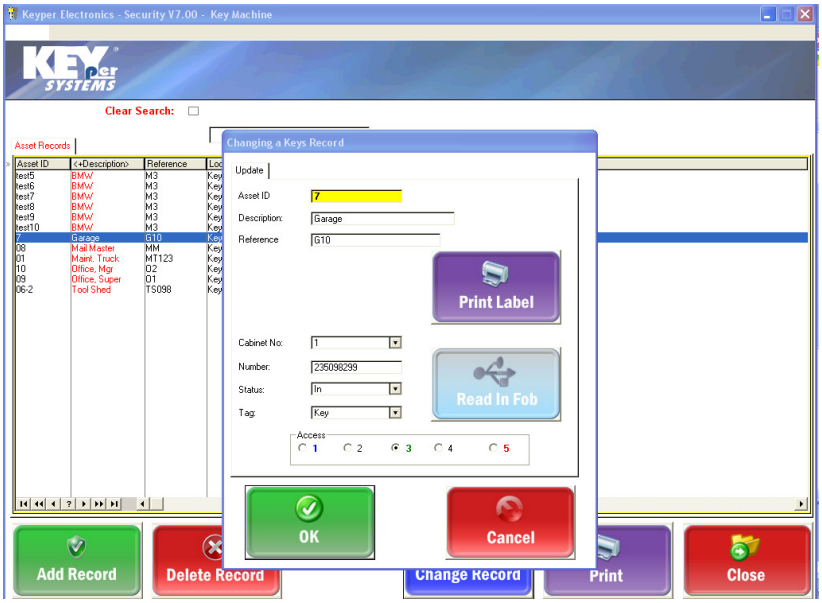


Fig. 9

!WARNING!

Any user with permission to* Admin *can change or delete any Asset!!

(See pg. 17, Set Operator Access)

Add an Asset (Login > Admin > Assets > Add Record)

(Figs. 10-11)

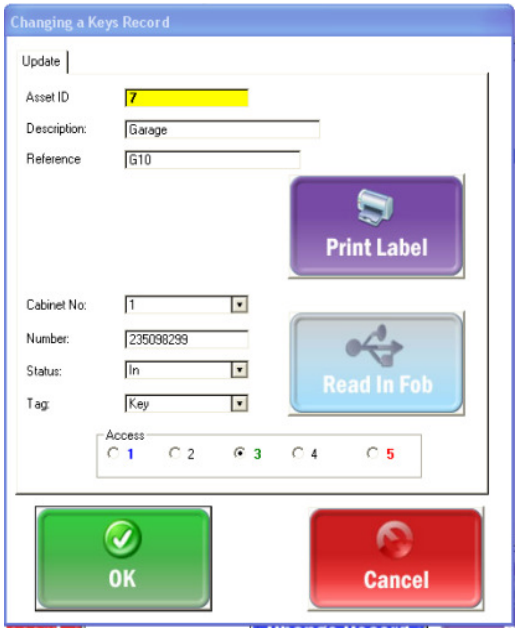


Fig. 10

The key(s) should be properly attached to the tamper seal and fob **(see pg. 5).** Select **Add Record** (**Fig. 9**) to bring up the screen in **Fig. 10**. Required fields are indicated with an asterisk. Begin by entering the vehicle **Asset ID** (ex., R110). This will be the most common search criterion. Enter a description (ex., Conference Room 110). A **Reference** is a kind of code that can be written on the asset itself but does not betray to what the asset actually allows access. The **Cabinet No:** field defaults to **1** and can remain so regardless of the cabinet into which the key will be placed. The location of the key will be detected by the system. Place the fob on the fob reader and click **Read In Fob** and the **Number** field will auto-fill**. Status** will remain **Out** until the key has been placed in a cabinet and "learned" into the system. **Access** will default to **3** unless otherwise specified.

***SECTION II*: *File Menu* (Login > File)**

Backup Scheduler (Login > File > Backup Scheduler)

(Fig. 11)

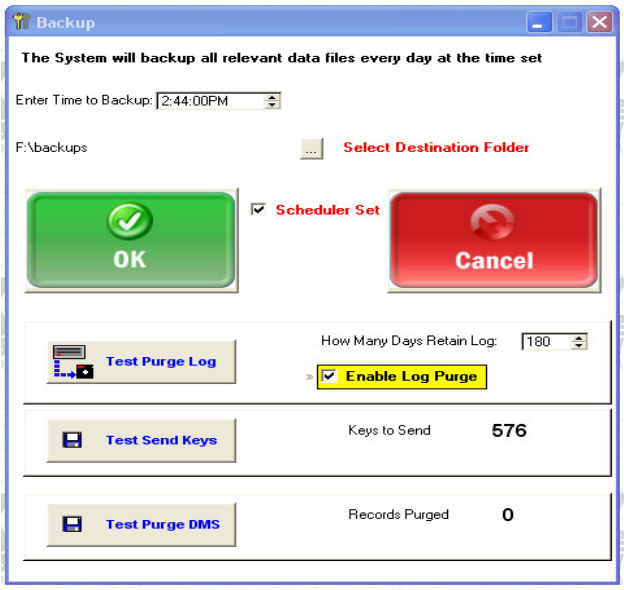


Fig. 11

The **Backup** feature copies and saves important data, once per day, to the backup drive supplied with your system, normally a removable USB drive. Backup settings are configured at time of installation but it is very important to ensure the backup scheduler is properly set. Enter the time at which the backup is to occur, click **Select Destination Folder** to choose where the data will be stored, enable **Scheduler Set** and click **OK**. The auto purge option will purge the audit log of records older than the number of days set in the **How Many Days Retain Log** window**,** select the number of day's of data to always have accessible and activate **Enable Log Purge**. The example in figure 7 instructs all log records older than 180 days be purged.

!WARNING!

Purged data is not retrievable

Issue Reasons (Login > File > Comport/Issue Reasons)

(Fig. 12)

Note: The **Serial Port** entries on this screen are preset at the factory and should not be changed.

If it is desired to require users to provide a reason when checking out an asset, ensure **Issue Reason Required** is checked. Check **Allow Multi-Checkout** to allow for one reason to be applied to a multi-asset check out. If activated, an **Issue Reason** screen will pop up during the **Check Out** procedure.

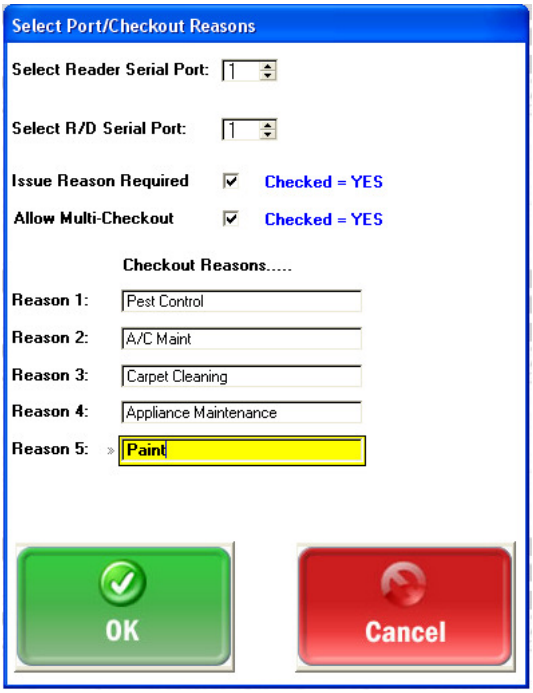


Fig. 12

Login Options (Login > File > Login Options)

(Fig. 13)

Select preferred log in option:

- Password Only.
- Biometric (Finger Print) Only.
- Biometric or Password.

The most secure login method is **Biometric**. A password can be shared, stolen or even guessed, but a fingerprint is virtually impossible to compromise.

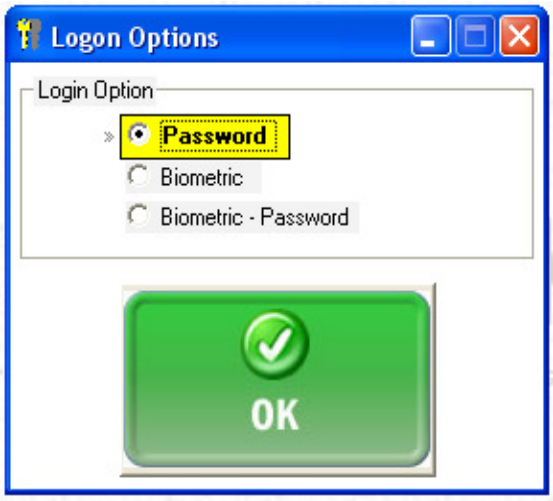


Fig. 13

Network Settings

This screen applies only to those **KEYper®** systems that are networked with other **KEYper®** systems. Network settings are usually configured at the time of system installation. These settings should not be altered without the knowledge and assistance of the key system administrators and **KEYper® Systems Technical Support**. Each system will have a set daily back-up time, after which each system will broadcast its' key data to the other systems. Therefore it is important that no system backup schedules overlap. A 30 minute difference between scheduled backup times is usually sufficient.

Print Setup

If your system is configured for printing, use this screen to select the desired printer and properties. Printers can be added to this computer through normal Windows procedures. Contact your IT department to add printers.

Purge Log File (Login > File > Purge Log File)

This function performs a "manual" purge of your log file. This can be done in addition to the automatic purge function discussed on **page 12** under **Backup Scheduler**. **Start Date** & **End Date** calendars are accessed by clicking on the respective calendar button. You must click on a date to exit the calendar. Depending on the expanse of the date range, purges can take several hours.

!WARNING!

Purged data is not retrievable

Set Email/Reports

Your system features two email options. One or both can be enabled. The **Keys Out Report** option provides an automatic, at the time of your choice, once daily, email report listing all keys checked out of the system as of the time of the email. The other option will send an email anytime an **Illegal Key Removal** has been detected. An illegal removal is triggered by a key and/or fob being removed without having been properly checked out. There can be multiple recipients for emails. This option is normally configured at the time of system installation. If your emails have not been configured or are not working, contact **KEYper® Systems Technical Support** for more information.

Test Email (Login > File > Test Email)

(Fig. 14)

Click **Test Keys Out** to send a test keys out report. Click **Send** to test the illegal removal warning email. Successful tests are self-evident, as are failed tests. If an error occurs contact your IT department.

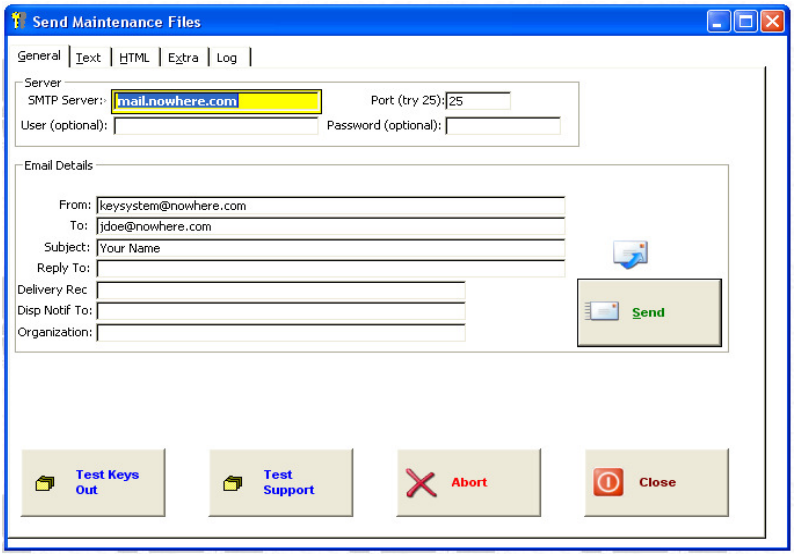


Fig. 14

Test System Communications

The functions under this sub-menu are for troubleshooting and diagnostic tasks. These functions should only be utilized by, or under the direction of, **KEYper® Technical Support**.

Time Outs/Settings (Login > File > Time Outs/Settings)

All time entries are in seconds. They are established at the time of system installation and are rarely altered. **Test Assets, Network Delay, Network Rebroadcast, Com Delay** and **Learn** entries should not be altered without the knowledge and approval of **KEYper® Technical Support**. **Settings** are not accessible to users.

Exit Application (Login > File > Exit Application)

This is the proper way to close the **KEYper®** software.

SECTION III: Supervisor Menu (Login > Supervisor)

This menu contains functions related to users

Access Profile (Login > Supervisor > Access Profile)

(Fig. 15)

Access Profiles are assigned to users when added to the system. The profile dictates what hours of the week and/or weekend a user may access the system. Click on **Add Record** and the inset screen appears. Name the profile, indicate **Week Day** and/or **Week End**, and enter **Start** & **End** times (12hr or 24hr clock formats accepted). **Fig. 15** dictates that users assigned the **Day Shift** profile can access the system from **8AM** until **5PM** on **Week Days** only.

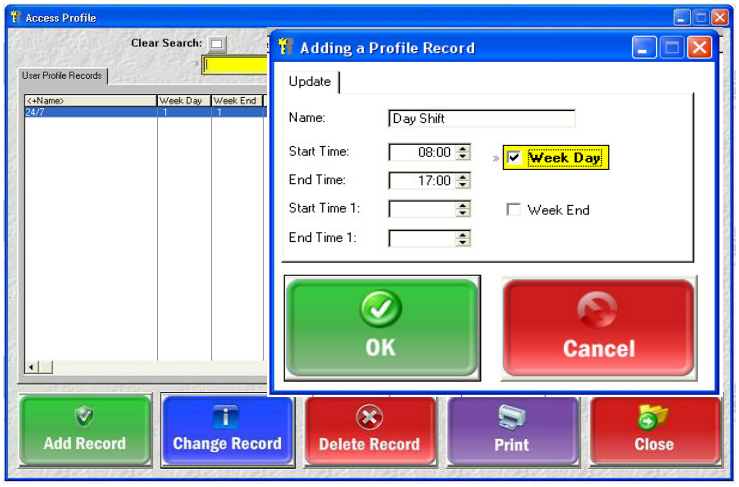


Fig. 15

Change Password (Login > Supervisor > Change Password)

This is the ***only*** proper function to use in order to change a password. The user requiring a password change ***must*** be the user logged into the system and must know their old password. If the user does not have permission to the **Supervisor** menu, then the user must be given that permission to change his/her password. After the password change has been accomplished, permission to the **Supervisor** menu can be removed. **(See Set Operator Access, pg. 17)**

Company (Login > Supervisor > Company)

To add a company to the **Company** database, select **Add Record**, enter the company information (only the company name is required) and click **OK.**

Department (Login > Supervisor > Department)

To add a **Department** to the database, select **Add Record**, enter the department name and click **OK.**

Group (Login > Supervisor > Group)

To add a **Group** to the database, select **Add Record**, enter the group name and click **OK.**

MAC Address

These entries are set at the time of installation and should not be altered without the knowledge and approval of **KEYper® Technical Support**.

Adding cabinets to an existing system (Login > Supervisor > MAC Address) (Fig. 16)

The cabinets in multi-cabinet systems are linked with Ethernet cables (CAT V), the ports for which, in most cases, are located at the bottom of the cabinet. The cable should be connected between RJ45 ports on the add on cabinet and the preceding cabinet. Once the Ethernet cable(s) is in place, connect the cabinet's power cord to a suitable outlet, preferably in a surge protected battery back up or multi-outlet strip. Navigate to the **MAC Address** window and select **Add Record**. The automatic entry in **Cabinet Number** is based on current entries should reflect the next number in order. If necessary, you can enter the correct number. The **Cabinet Address** number can be obtained from the sticker on the door of the new cabinet. Enter this number in **Cabinet Address**. Next enter the number of key positions in the new cabinet (40, 80, 160, etc) in **No. Key Slots**. If any of the positions in the cabinet are reserved for dealer plates, enter that number in **No. Tag Slots**. Select **OK**, then **Close.** For a quick test, log in and select **Check In**. You should see a window allowing you to choose which cabinet to open. If you do not see the cabinet you just added or if there are any issues, please contact **KEYper® Support.** (800.399.7888)

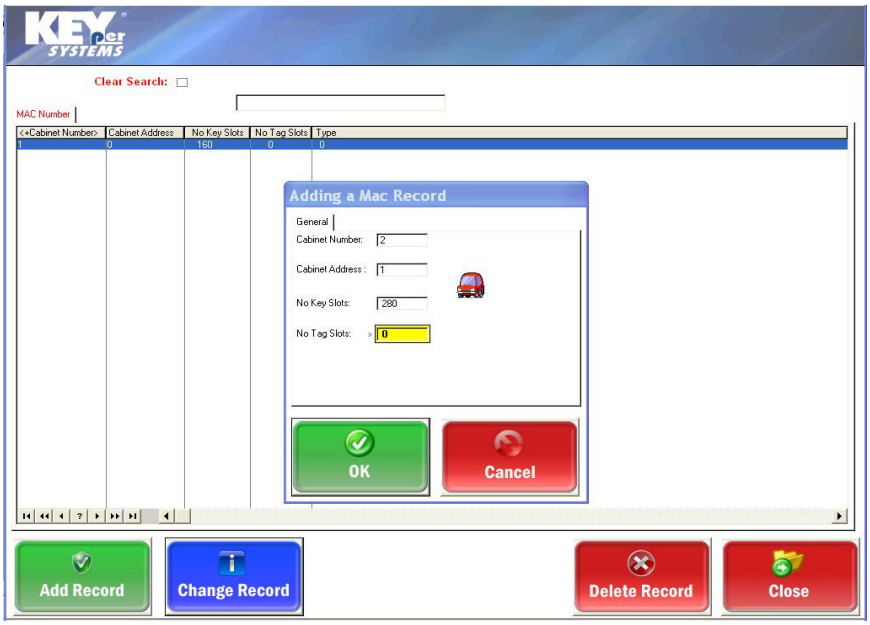


Fig. 16

Set Operator Access **(Login > Supervisor > Set Operator Access)**

(Fig. 17)

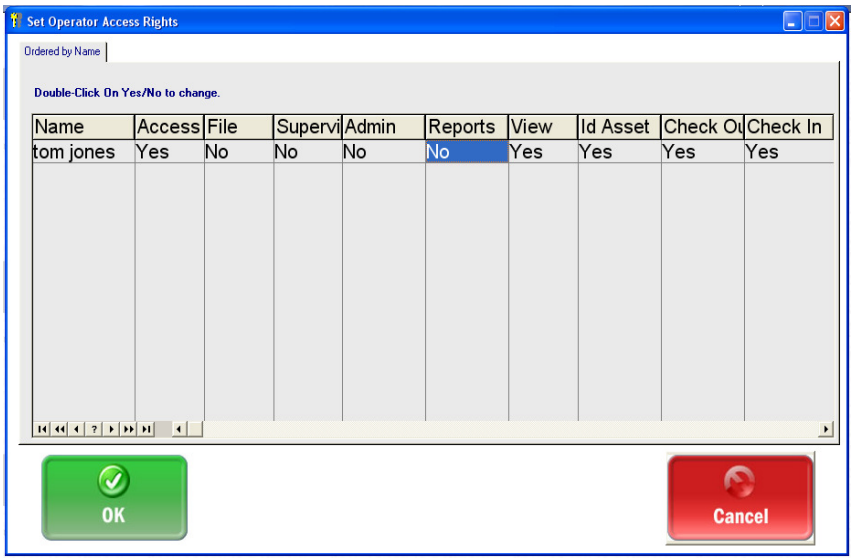


Fig. 17

It is ***very important*** that at some point users permissions be established, whether after several users are loaded or after each user is loaded. Only users entered as **Operators** are displayed. Users entered as **Supervisors** have full system access by default and do not appear in this database. Control a user's access to various areas by double clicking on **Yes** or **No** to change the value. **Remember!!** If an operator is given access to **Supervisor**, for instance, that operator has access to ***everything*** in the **Supervisor** menu. Be careful who gets access to what.

Position **(Login > Supervisor > Position)**

To add a **Position** to the database, select **Add Record**, enter the position name and description, if desired, and click **OK.**

Users **(See pg. 9 for adding or deleting users)**

Access Level…The thing to remember here is the relationship between a user's access level and key access levels. A user can legally check out only those keys equal to or less than the user's assigned **Access Level**. For example, if you are assigned **Access Level 3** you cannot "legally" access a key that has been assigned an **Access Level 4** or **5**. If no **Access Level** is selected, the system will automatically assign **Access Level 3**. This default is most commonly used for **Operators** while **Supervisors** are usually assigned level 5. The same is true of key access levels.

SECTION IV: ***Admin Menu*** **(Login > Admin)**

This menu contains functions related to keys.

Configure Key Cabinets **(Login > Admin > Configure Key Cabinets)**

This command forces the system to recheck, or to "learn" again, the key inventory in the cabinet. You can force this "re-learn" if it appears the system is in error with regard to the number of keys checked out.

Import **(Login > Admin > Import)**

This function allows the importation of an asset, or keys, file directly into the assets database. However, the file ***must*** be converted into a .csv format for the import to function properly.

Assets **(See pg. 11 for Adding or Deleting Assets)**

Searching Assets Database (Fig. 18)

It is important to understand the sorting and searching features of the **Assets** database and window. First, a column is highlighted in **red** by clicking on a column header, such as **Description**. That tells the system to sort the asset database by **Description** *and* the search criterion is now based on asset description. That is to say, with a search criterion of **Description**, search entries ***must*** be a description**.**

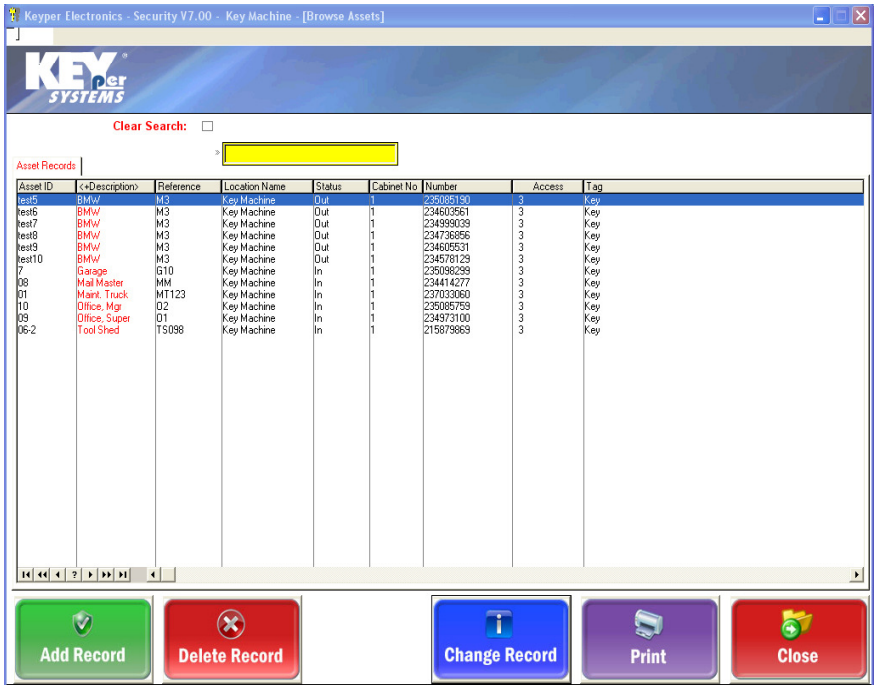


Fig. 18

If the **Reference** column is in **red**, search entries must be reference codes. The computer is going to search the highlighted column for whatever is entered in the search bar. Type an entry relating to the highlighted column into the yellow search bar and press **Enter**.

Remove Unknown Fobs **(Login > Admin > Remove Unknown Fobs)**

(Fig. 19)

An "**Unknown Fobs Found**" message in the upper right area of the toolbar indicates there are one or more fobs in the cabinet(s) that has not been entered in the keys database. Click on **Issue Keys** to fire the cabinet and light the unknown fobs. Once you have removed the fobs and closed the cabinet door, allow the system to configure and return to the log in screen. ***Do not click on*** **Cancel*!!***

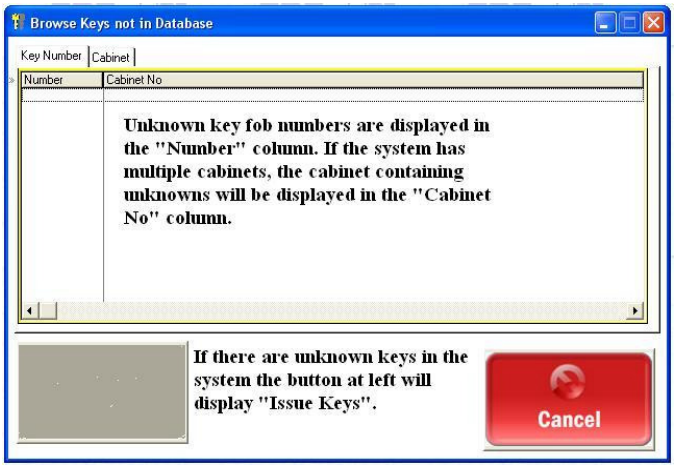


Fig. 19

SECTION V: Views Menu (Login > View)

View Audit (Login > View > View Audit)

This is your log file. All **Check Out** and **Check In** transactions are recorded here. Also recorded are key additions and deletions.

View Assets (Login > View > View Assets)

This screen allows you to view your assets database. This is ***view only!*** No changes can be made to the database on this screen.

View Assets In (Login > View > View Assets In)

This screen displays a list of assets currently in the cabinet.

View Assets Out (Login > View > View Assets Out)

This screen displays a list of assets currently checked out, who checked them out and when they were checked out.

View Assets Out by Days (Login > View > View Assets Out by Days)

Use this option if you need to delete assets from inventory but no longer have the fobs.

View Users (Login > View > View Users)

This screen allows you to view your user database. This is ***view only!*** No changes can be made to the database on this screen.

SECTION VI: Reports Menu **(Login > Reports)**

Daily Transaction Report **(Login > Reports > Daily Transaction Report)**

(Fig. 20)

Click on the calendar button to bring up the screen shown in **Fig. 20**. Select a date and click **Print** and any information for the selected date will be presented. Click on the printer icon in the upper right corner of the next window to print a hard copy of the report.

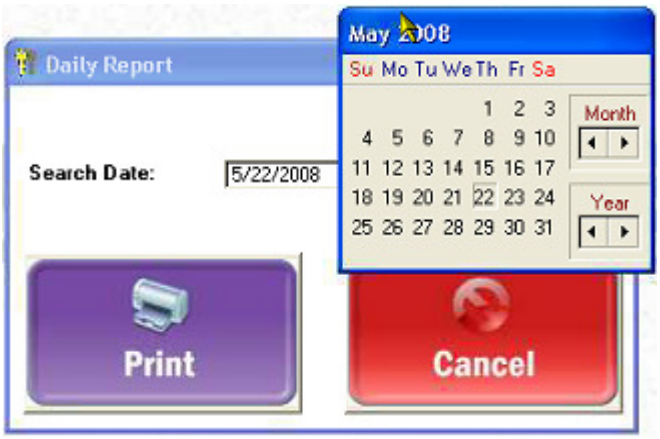


Fig. 20

Export Asset Data **(Login > Reports > Export Asset Data)**

(Fig. 21)

The information in the keys database can be exported and read in an Excel format. The key system controller is not loaded with, nor should be loaded with, any office type software. Remember, the key system controller is to be used explicitly for the operation of the key system. Loading software without the knowledge and consent of **KEYper® Systems** will nullify any system warranty. If the key system is on a network, the key data can be exported to a computer with office software. Choose which keys to export; status **In**, **Out** or **All**. If the system is networked, choose from where the keys will be exported; either from the local system only or from all networked systems. Select where the exported key data will be received. Click **Go**.

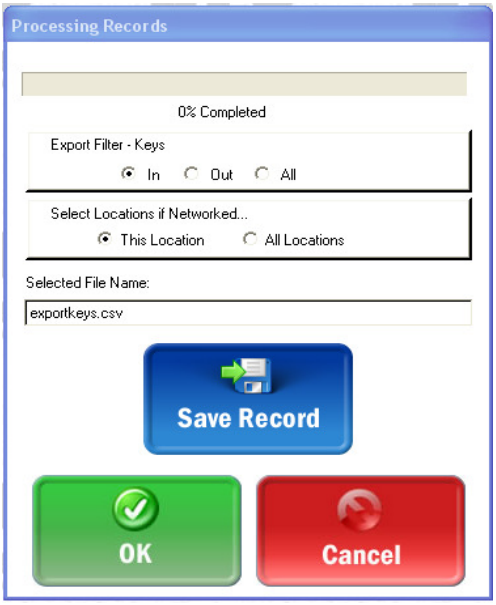


Fig. 21

User History (Login > Reports > User History)

(Fig. 22)

To view a user's history for a given time period, highlight the users name, click the **Select Date** buttons and set your desired start and end dates. You can also choose to see a complete history for all users. Click **Print** to view history. If your system is configured with a printer, click on the printer icon in the upper left corner of the next screen to print a hard copy of the report.

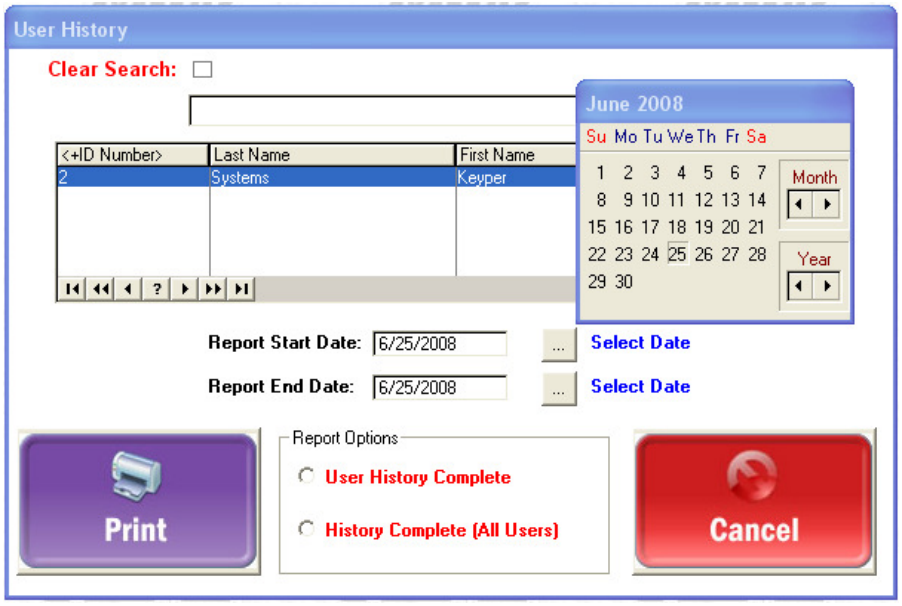


Fig. 22

Asset History (Login > Reports > Asset History)

This function works very much like **User History**. Select an asset, enter a date range and click **Print**. If your system is configured with a printer, click on the printer icon in the upper left corner of the next screen to print a hard copy of the report.

SECTION VII: Troubleshooting

If a question or system error is not addressed or if any of the following fail to correct an issue, please contact **KEYper® Technical Support** for assistance.

1-800-399-7888 or 704-455-9400 Mon – Fri 8:00 AM – 5:00 PM EST

After hours tech support 704-507-3147

! All of the following procedures should be performed by key system administrators !

1E: ***The system is frozen, locked up, stuck, looping, or otherwise not responding.***

1A: It is rare for the system program to actually freeze or lock up. Very often what has occurred is a timeout error, from which the system will recover after several minutes. Timeouts can be caused by shorted electronics in the cabinet or by disruptions in system communication. Timeouts can also be triggered by a user leaving a cabinet door open too long or waiting too long to open a cabinet door. If this occurs it is preferred to let the system recover on its own. If this is not possible or if after several minutes the system has not recovered, press **Ctrl>Alt>Del** and bring up the task manager. **(See fig. 23)**

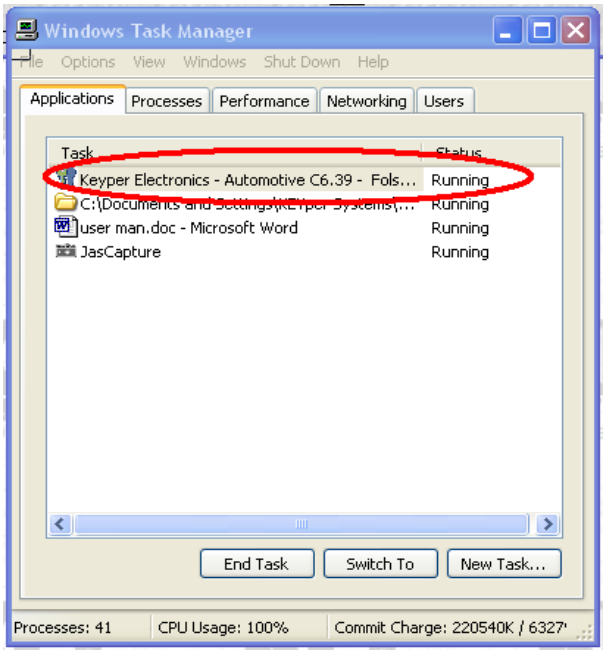


Fig. 23

Highlight the **KEYper® Electronics** application and select **End Task**.

Select **End Now** from the next window.

Restart the **KEYper®** software and log in to initiate a system configuration. It is recommended that, after the system configuration is complete and the log in screen returns, a **Configure Key Cabinets** function be accomplished. **(See pg. 18)**

2E: ***The cabinet clicks repeatedly, but does not open.***

2A: While the cabinet is clicking, manually open the cabinet door with the key that fits the cylinder lock on the door face, known as the "Hard Key". One or more key positions in the cabinet will likely be steadily illuminated, or "hard lit". Whether or not there are keys in any of these positions is of little consequence. Choose a starting point and ***one at a time***, manipulate the spring loaded "blue dot" with a finger or pencil eraser, until the cabinet stops clicking. Place a strip of tape over that position to prevent its use. With the door open, unplug the cabinet from its power source for 30 seconds, and then reconnect the plug. There should be an audible click, the large LED in the top left corner of the cabinet should flash after which 3 short beeps will indicate the cabinet has successfully reset. Finally, perform **Configure Key Cabinets**. **(See pg. 18)**

3E: ***User receives an* Invalid Login *or other errors during log in.***

3A: The likely cause is a user that was deleted from and then re-added to the user database without a name change. Delete and re-add the user as instructed beginning on **pg. 9**.

4E: ***User is having difficulty or cannot login with the fingerprint reader.***

4A: Reprint the user as instructed beginning on **pg. 10**.

5E APPLIES TO SYSTEMS CONFIGURED WITH RF COMMUNICATIONS ONLY!!

5E: ***All keys have a status of 'OUT'.***

5A: The likely cause is a disruption in system communication. Unplug cabinet(s). Ensure the desktop radio is connected securely and that there is one red and one green light illuminated on the radio. Ensure all radio antennas are in place and not damaged. Re-connect the cabinet(s), ensure the cabinet(s) reset successfully (3 beeps within 60 seconds of re-connecting). Finally, perform **Configure Key Cabinets**. **(See pg. 18)**

6E: ***Errors when adding keys.***

6A: There are two errors that can occur when programming assets into the system. Read the error message carefully. One error will arise when the fob being used is associated with another asset. Perform an **Identify Fob** function on the fob to determine if that fob is still associated with another asset. If so, either use a different fob or delete the asset. The other error arises from the fact that the asset being entered is already in the system. To determine if this is the case, go to the **Assets** database and search for the asset. **(See pg. 18)**

7E: ***Fob does not read.***

7A: Inspect the fob for damage, particularly the button face. A dented fob button may read when placed on the fob reader but not when placed in the cabinet.

8E: ***Fob Reader does not read fobs.***

8A: **IMPORTANT: The fob reader should be connected to the powered USB hub provided with the system for normal operation.** Close the **KEYper®** software. Disconnect the fob reader, which includes the blue USB adapter, from its current USB port and connect into another USB port. If this resolves the issue, a "*Found New Hardware Wizard"* window will appear. In this window select the *"No, not this time"* option and click next. The correct option will be pre-selected in the next window; make no changes; click next. The system will load the drivers for the fob reader. Follow all screen directions, allow the task to complete. Reboot the system controller, open the **KEYper®** software and check the operation of the fob reader. If the issue is not resolved, repeat the procedure for any other open USB ports.

9E: ***User cannot check out assets; "Issue Limit Reached" error.***

9A: The main cause of this error is lack of proper maintenance to the assets out database. See **View Assets Out**. Ensure the user's issue limit has not been exceeded. If necessary, adjust user's **Issue Limit** or **No. Issued**. **(See pg. 9, Fig.5)**

CABINET MAINTENANCE

!! Always remove power from the cabinet before performing an maintenance !!

In figure 24 are pictured the minimum tools recommended to perform basic cabinet maintenance

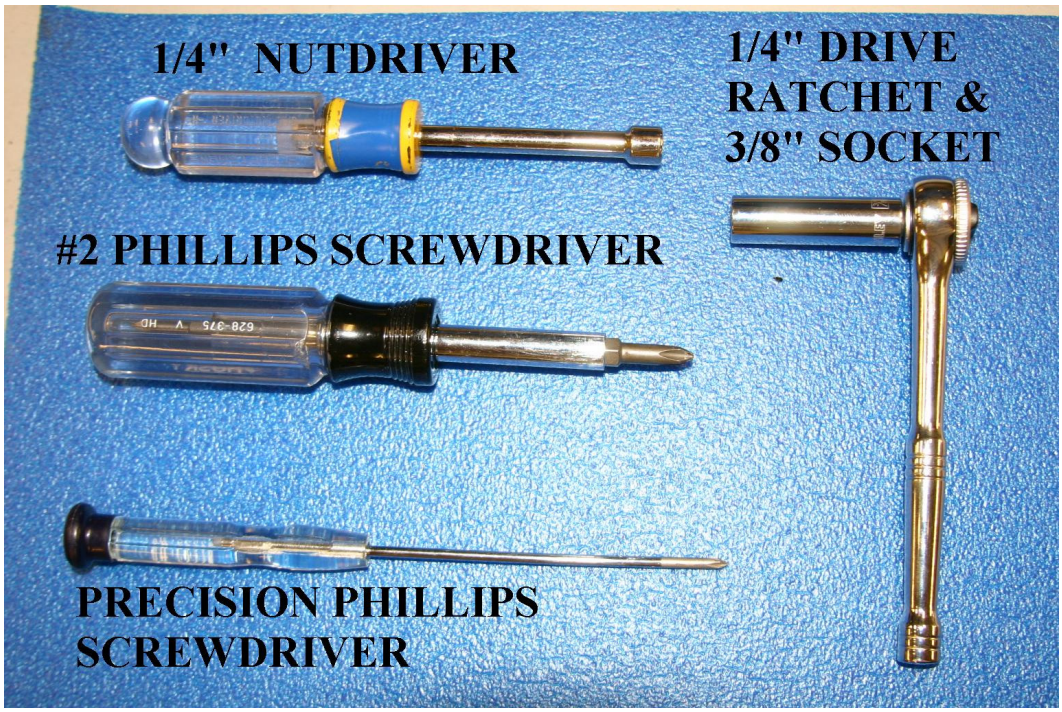


Fig. 24

40 POSITION PANEL REMOVAL & INSTALLATION

Each 40 position panel is held in place by four(4) 3/8" hex head bolts, one in each panel corner. Using a ratchet and socket, or other appropriate wrench, remove the bolts. Be sure to support the panel as the last bolt is removed. **CAUTION: take extreme care to ensure the wire leads connected to the back of the panel do not get hung on other wires as the panel is removed.** Gently remove the panel, turn it vertically, right side up, and rest the panel in the bottom of the cabinet. Disconnect the Molex connector to the panel and remove the panel from the cabinet. **See figures 25 - 30.**

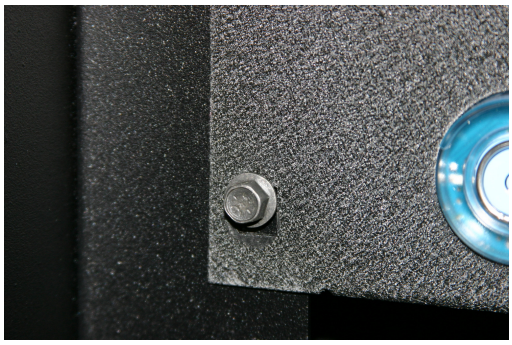


Fig. 25

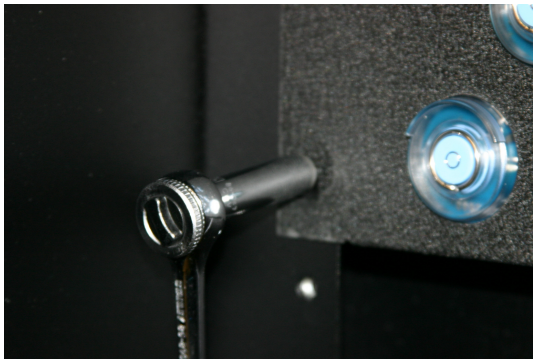
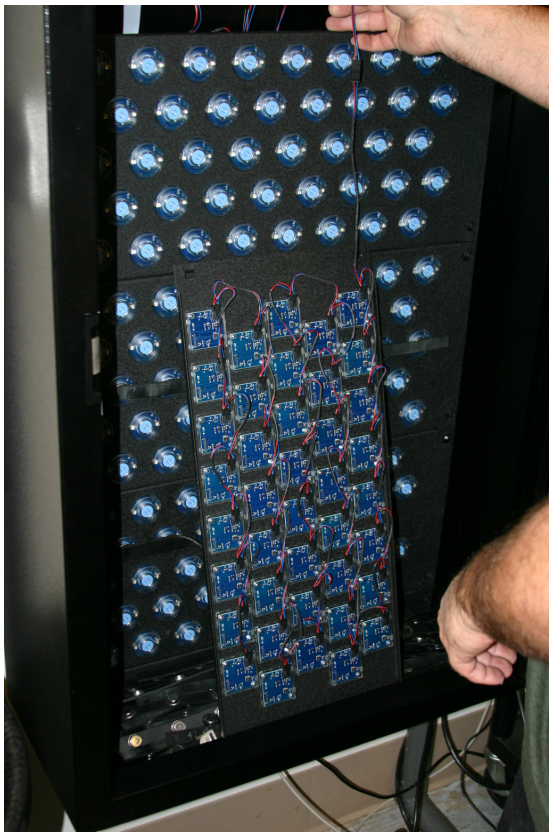


Fig. 26

Fig. 27

Fig. 28



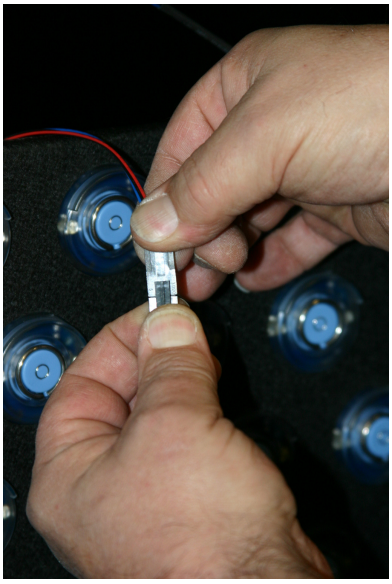


Fig. 29

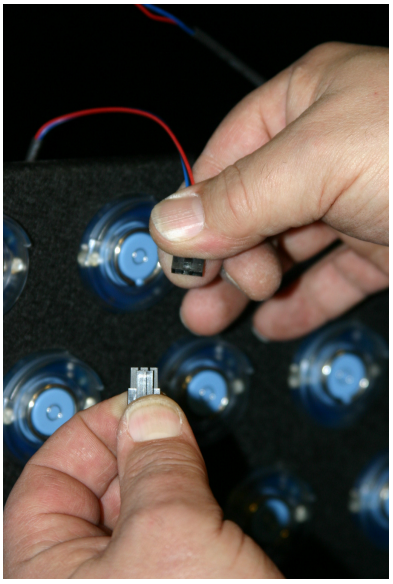


Fig. 30

The procedure for installation of the panel is basically a reversal of the previous actions.

CAUTION: ensure no wires are pinched, nicked or otherwise damaged upon installation

CAUTION: *REMOVE POWER FROM THE CABINET BEFORE PERFORMING ANY MAINTENANCE*

DOOR PANEL REMOVAL & INSTALLATION

CAUTION: it is highly recommended the following procedures be performed by two(2) people

If the door panel is being removed for reader board assembly or wiring replacement, follow the procedure in paragraph **A** below and refer to **figures 31-33**.

If the door panel is being removed for replacement, follow the procedure in paragraph **B, pg. 31.**

A. Door panel removal for RBA replacement

1. with one person supporting the panel remove the corner screws (4). **(Figs. 31-32)**
2. gently swing the panel toward the cabinet interior and let it rest on the door frame. Keep the panel supported as long as it is in this position. **(Fig. 33)**
3. replace RBA(s) as required.
4. to re-install panel – one person supports the panel in position on the door while a second person installs the corner screws. Do not over tighten screws! "Snug" is fine.

Fig. 31

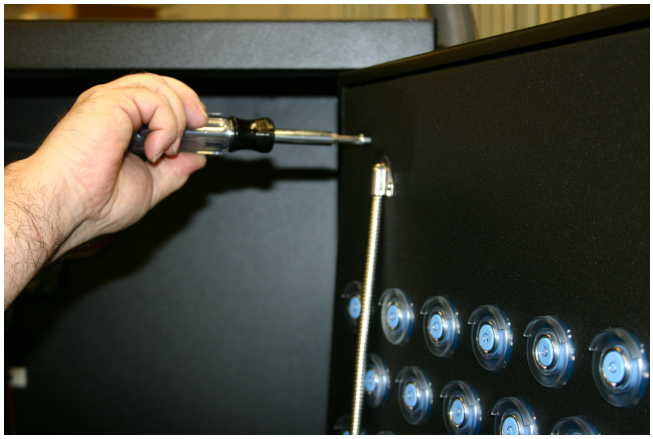


Fig. 32

Once the mount screws have been removed, gently swing the panel toward the cabinet interior and rest it on the bottom of the door frame.

<u>The panel must remain supported while in this position !!!</u>

While one person supports the panel, another can perform the maintenance.

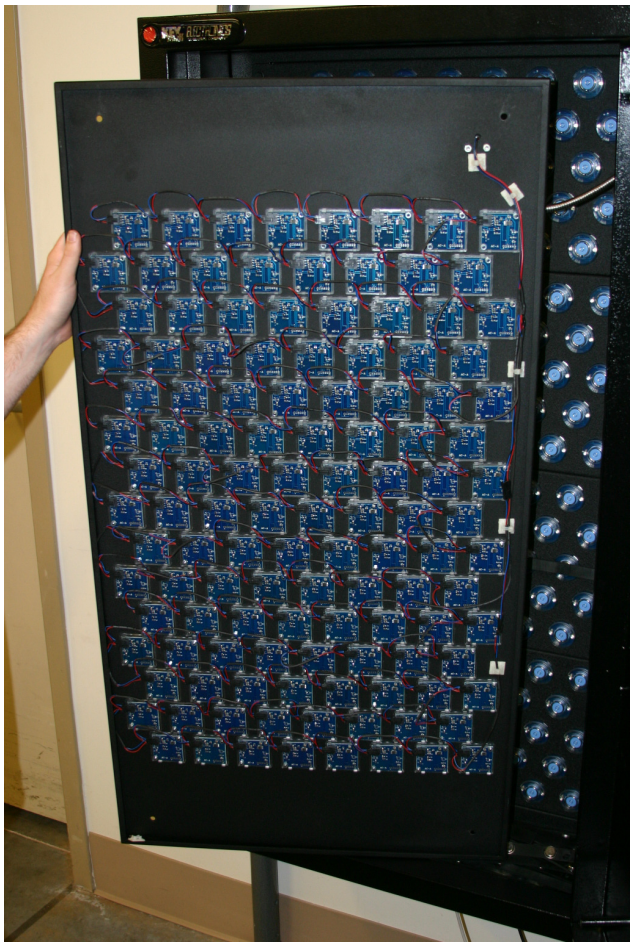


Fig. 33

CAUTION: *REMOVE POWER FROM THE CABINET BEFORE PERFORMING ANY MAINTENANCE*

B. Door panel replacement

B1. Removal

1. remove the top interior panel as described on page 27.
2. disconnect the door leads from the controller. **(Fig. 34)**
3. remove the 3/8" hex head bolts (2) from the spacer at the top of the cabinet. The door panel, the spacer, the flexible conduit and the door panel leads all stay together. **(Fig. 35)**
4. with one person supporting the panel remove the corner screws (4) and lift the panel with spacer, flex conduit and leads away from the door.

B2. Installation

5. with one person supporting the panel install the corner screws (4). Do not over tighten screws! "Snug" is fine. **(Figs. 31-32)**
6. place the spacer into position and install bolts ***finger tight!***
7. connect the door panel leads to the controller. ***Ensure all wire leads are secure!*** **(Fig. 34)**
8. install the top interior panel, tighten all 3/8" hex head bolts.

CAUTION: ensure no wires are pinched, nicked or otherwise damaged upon installation

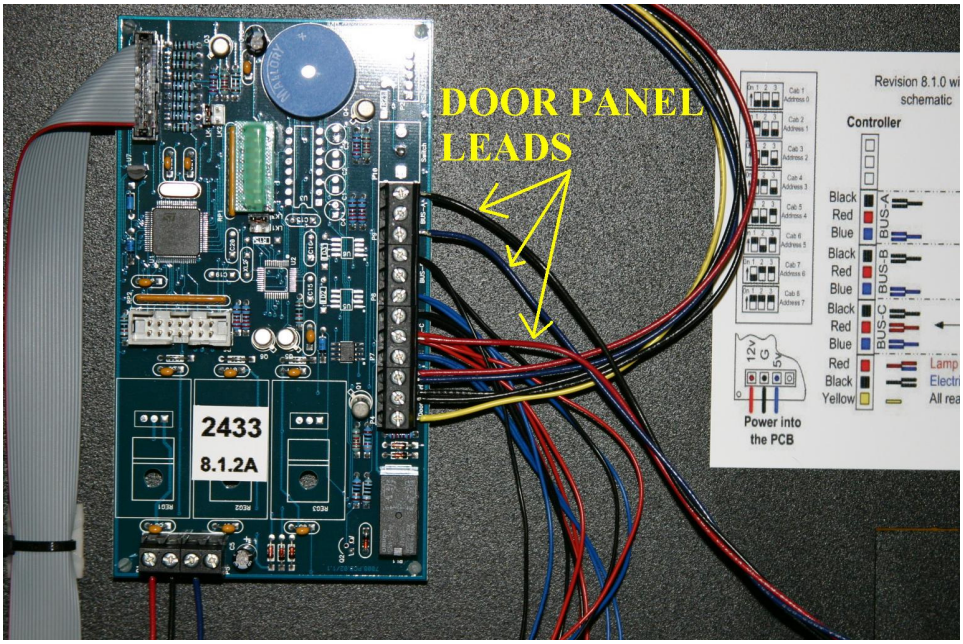


Fig. 34

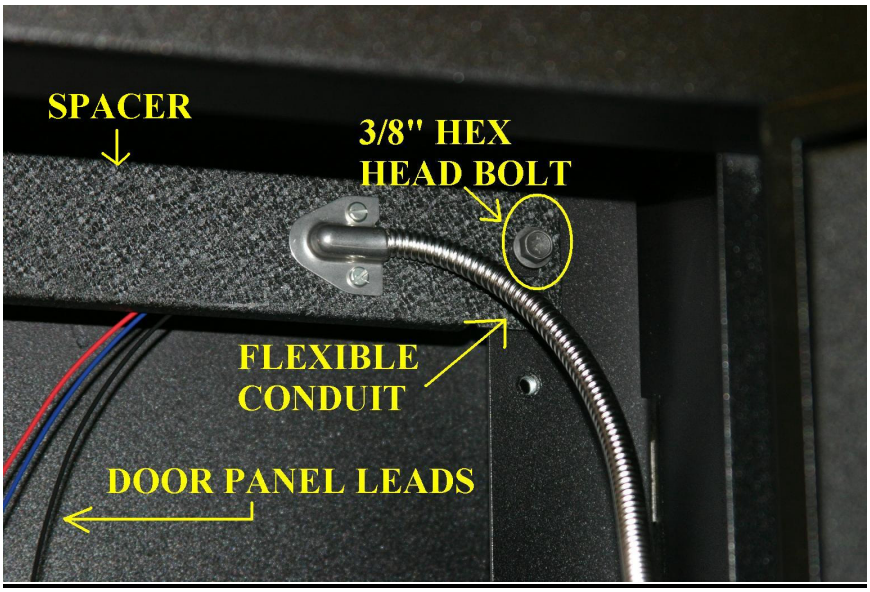


Fig. 35

CAUTION: *REMOVE POWER FROM THE CABINET BEFORE PERFORMING ANY MAINTENANCE*

READER BOARD ASSEMBLY (RBA) REMOVAL & INSTALLATION

A reader board assembly consists of three parts; the reader board, the lens and the "blue-dot", as seen in figure 36. *Note: the lens and blue-dot sub-assembly are pictured from the back.*

Replacement RBA's are shipped fully assembled.

If you are replacing RBA's in the 40 position panels, *remove the panels as described beginning on page 27.*

If replacing door panel RBA's, *remove the panel as described beginning on page 31*.

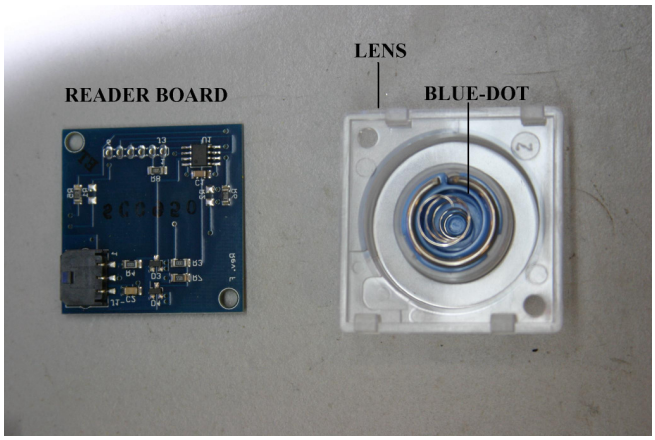


Fig. 36

RBA Removal and Installation **(Fig. 37)**

Once the appropriate panel is removed, disconnect the Molex connector from the defective RBA. Remove two(2) ¼" nuts from RBA and remove RBA from panel. Position replacement RBA in panel, attach with two(2) ¼" nuts lightly tightened and reconnect Molex. Install panel into cabinet in accordance with instructions on pages 27-34.

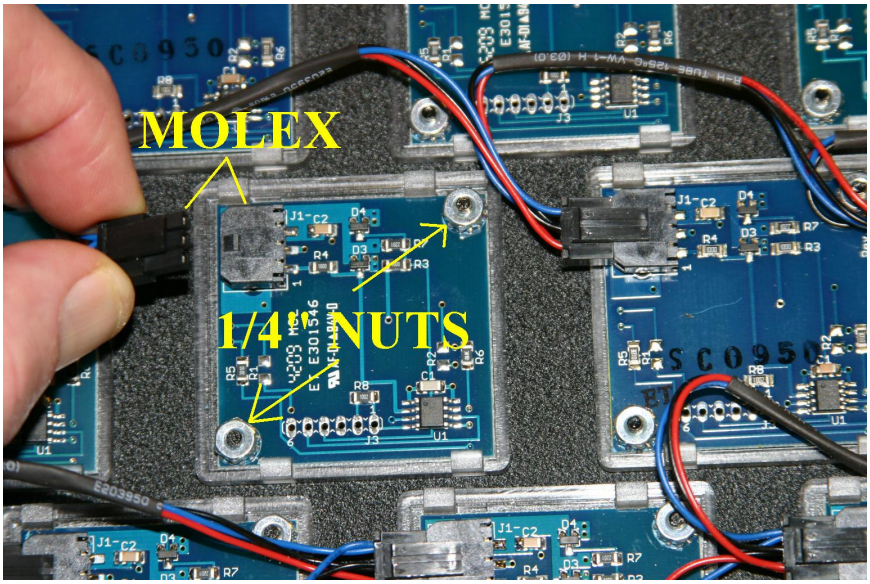


Fig. 37